Variations on Minimal Linear Codes

Gérard Cohen[1] and Sihem Mesnager[2]

[1]Institut Télécom, Télécom ParisTech, UMR 7539, CNRS. E-mail: cohen@telecom-paristech.fr
[2]LAGA (Laboratoire Analyse, Gometrie et Applications), UMR 7539, CNRS, Department of Mathematics, University of Paris XIII and University of Paris VIII, Sorbonne Paris Cité. E-mail: smesnager@univ-paris8.fr

Abstract. Minimal linear codes are linear codes such that the support of every codeword does not contain the support of another linearly independent codeword. Such codes have applications in cryptography, e.g. to secret sharing. We pursue here their study and construct asymptotically good families of minimal linear codes. We also push further the study of quasi-minimal and almost-minimal linear codes, relaxations of the minimal linear codes.

1 Introduction

A *minimal codeword* [Mas93,Mas95] c of a linear code C is a codeword such that its support (set of non-zero coordinates) does not contain the support of another linearly independent codeword. Minimal codewords are useful for defining access structures in secret sharing schemes using linear codes. Determining the set of minimal codewords is hard for general linear codes, although this has been studied for some classes of specific linear codes. This led to work on how to find codes where all codewords are minimal, in order to facilitate the choice of access structures. The problem of finding a code satisfying this condition, called a *minimal linear code* has first been envisioned in [DY03] and later studied in [SL12,CCP13].

Interestingly, in [CCP13], the motivation for finding minimal linear codes is no longer secret sharing but in a new proposal for secure two-party computation, where it is required that minimal linear codes are used to ensure privacy.

It is pointed out in [CCP13] that minimal codes are close to the notions of intersecting and separating codes [CL85,CELS03]. Such codes have been suggested for applications to oblivious transfer [BCS96], secret sharing [AB98,DY03,SL12] or digital fingerprinting [Sch06].

We will focus here on the non-binary case, where the notion of minimal codes is more restrictive than that of separating codes. Secret-sharing and secure two-party computations both crucially hinge on a large alphabet; thus, one cannot rely on the well-understood binary case only.

We thus pursue in Section 2 the study of [CCP13] on bounds and criteria for minimal linear codes and exhibit families of minimal codes with better rates (asymptotically non-zero). In Section 3, we relax the notion of minimal codes and introduce *quasi-minimal* linear codes. Quasi-minimal linear codes are codes where two non-zero codewords have the same support if and only if they are linearly dependent. This slight relaxation enables to exhibit families with improved non-zero asymptotic rates. Finally, we consider yet another generalization to almost-minimal codes, where the property is allowed to fail for a small proportion of codewords.

2 Minimal Codes – Bounds and Constructions

2.1 Definitions – Notations

We denote by $|F|$ the cardinality of a set F. Let $q = p^h$, where p is a prime number and $h \in \mathbb{N}*$. An $[n, k, d, d_{max}]_q$ code is a vector subspace of $\mathbb{F}_q^n$ of dimension k with minimum distance d and maximum distance d_{max}.

The last two parameters refer to the minimal (resp. maximal) Hamming distance between two codewords of $\mathcal{C}$, or, equivalently, the minimal (resp. maximal) Hamming weight of a codeword of $\mathcal{C}$; they will be omitted when irrelevant. Normalized parameters will be denoted by $R = k/n, \delta = d/n, \delta_{max} = d_{max}/n$.

The *support* of a codeword $c \in \mathcal{C}$ is $supp(c) = \{i \in \{1, \ldots, n\} | c_i \neq 0\}$. The *Hamming weight* of a codeword $c \in \mathcal{C}$ denoted by $wt(c)$ is the cardinality of its support : $wt(c) = |supp(c)|$. A codeword c *covers* a codeword c' if $supp(c') \subset supp(c)$.

Definition 1 (Minimal codeword). *[Mas93] A codeword c is minimal if it only covers $\mathbb{F}_q \cdot c$, i. e. if $\forall c' \in \mathcal{C}, (supp(c') \subset supp(c)) \implies (c, c')$ linearly dependent.*

Definition 2 (Minimal linear code). *[DY03] A linear code $\mathcal{C}$ is minimal if every non-zero codeword $c \in \mathcal{C}$ is minimal.*

For a complete treatment and general references in coding theory, we refer to the book of MacWilliams and Sloane [MS77].

2.2 Bounds

Two non-constructive bounds on the rates of minimal codes are exhibited in [CCP13]. We recall them without proofs.

Theorem 1 (Maximal Bound). *[CCP13] Let $\mathcal{C}$ a minimal linear $[n, k, d]$ q-ary code, then $R \leq \log_q(2)$.*

Theorem 2 (Minimal Bound). *[CCP13] For any R, $0 \leq R = k/n \leq \frac{1}{2}\log_q(\frac{q^2}{q^2-q+1})$, there exists an infinite sequence of $[n, k]$ minimal linear codes.*

2.3 A sufficient condition

There exists a sufficient condition on weights for a given linear code to be minimal. More precisely, if the weights of a linear code are close enough to each other, then each nonzero codeword of the code is a minimal vector as described by the following statement.

Proposition 1. *[AB98] Let $\mathcal{C}$ be an $[n, k, d, d_{max}]$ code. If $\frac{d}{d_{max}} > \frac{q-1}{q}$ then $\mathcal{C}$ is minimal.*

Remark 1. Note that the stronger sufficient condition $\frac{d}{n} > \frac{q-1}{q}$ fails to provide asymptotically good codes; indeed, by the Plotkin bound ([MS77], for any code, not necessarily linear, of length n, size M and distance d, if $d > (q-1)n/q$, then $M \leq d/(d-(1-q^{-1}))$.

On the other hand, for $\delta < 1 - q^{-1}$, the classical Varshamov-Gilbert bound [Gil52] guarantees the existence of asymptotic families of codes with non zero rate $R(\delta, q)$.

2.4 Infinite constructions

The general idea is to concatenate a q-ary "seed" or inner code (e.g. a simplex) with an infinite family of algebraic-geometric (AG) codes (the outer codes) [TV91], in such a way as to obtain a high enough minimum distance and conclude by Proposition 1.

In practice, we can take the seed to be the simplex code $\mathcal{S}_{q,r}[n = (q^r-1)/(q-1), k = r, d = d_{max} = q^{r-1}]_q$ (with $\delta > (q-1)/q$), set $r = 2m$ and concatenate with $AG[N, K = NR, D = N\Delta, D_{max} = N\Delta_{max}]_{q^{2m}}$. These codes exist lying almost on the Singleton bound, namely satisfying $R + \Delta = 1 - (q^m - 1)^{-1} > (q-1)/q$.

This concatenation results in the family $C[nN, kK, dD]_q$ with maximum distance at most $d_{max}N$. If $dD/d_{max}N = \Delta > (q-1)/q$, this family is minimal by Proposition 1.

It is not hard to check that, for example, choosing q large and α small enough, $m \geq 2, \Delta = (q-1)/q + \alpha, R = 1/q - 1/(q^m - 1) - \alpha > 0$, this is the case.

To summarize, we construct infinite families of codes with $R = 2m(1/q - 1/(q^m-1) - \alpha)(q-1)/(q^{2m}-1) \approx 2m/q^{2m}$ satisfying $\delta/\delta_{max} > (q-1)/q$, thus minimal. Note that, by the Plotkin bound, they necessarily satisfy $\delta < (q-1)/q$, so the fact that $\delta_{max} < 1$ is crucial.

3 Quasi-minimal codes

We now relax the notion of minimal codes to that of *quasi-minimal* codes. Minimality prevents a codeword from having its support included in the support of a linearly independent codeword, whereas quasi-minimality only prevents two linearly independent codewords from having the same support.

3.1 Definitions and Properties

Definition 3 (Quasi-minimal codeword). *A codeword c is quasi-minimal if $\forall c' \in \mathcal{C}, (supp(c') = supp(c)) \implies (c, c')$ linearly dependent.*

Definition 4 (Quasi-minimal linear code). *A linear code $\mathcal{C}$ is quasi-minimal if every non-zero codeword $c \in \mathcal{C}$ is quasi-minimal.*

Quasi-minimality is clearly a weaker requirement than minimality. For instance, every binary code is obviously quasi-minimal.

3.2 Constructions

We now give a construction based on the Kronecker (tensor) product of codes, which yields infinite families of quasi-minimal codes with relatively slowly decreasing rates.

Proposition 2. *The product $\mathcal{C}_1 \otimes \mathcal{C}_2$ of a quasi-minimal $[n_1, k_1, d_1, (d_{max})_1]_q$ code $\mathcal{C}_1$ and of a quasi-minimal $[n_2, k_2, d_2, (d_{max})_2]_q$ code $\mathcal{C}_2$ is a quasi-minimal $[n_1 \times n_2, k_1 \times k_2, d_1 \times d_2, d_{max} \geq (d_{max})_1 \times (d_{max})_2]_q$ code.*

Proof. The parameters are easy to check. For the quasi-minimality, let $c \neq 0, c'$ be two codewords of $\mathcal{C}_1 \otimes \mathcal{C}_2$. By definition of the tensor product, they can both be written as $n_1 \times n_2$ matrices where rows are codewords of $\mathcal{C}_1$ and columns are codewords of $\mathcal{C}_2$. More generally, the square of the $[q+1, 2, q]_q$ simplex code is a $[(q+1)^2, 4, q^2]_q$ minimal code. Let us assume that $supp(c) = supp(c')$. For $i = 1, \ldots, n_1$, $j = 1, \ldots, n_2$ let c_i^1 (resp. $c_i'^1$) be the i^{th} row of c (resp. c') and c_j^2 (resp. $c_j'^2$) be the j^{th} column of c (resp. c'). For every i, $supp(c_i^1) = supp(c_i'^1)$, so $\exists \lambda_i$ such that $c_i'^1 = \lambda_i c_i^1$. With the same reasoning on the columns, for every j, there exists λ_j such that $c_j'^2 = \lambda_j c_j^2$. Then, all the λ_i's and λ_j's are equal and there exists λ such that $c' = \lambda c$, so c and c' are linearly dependent. Thus, $\mathcal{C}_1 \otimes \mathcal{C}_2$ is quasi-minimal. □

3.3 A sufficient condition

We now prove a sufficient condition for quasi-minimality, weaker than the one for minimality. This will then allow us to construct improved infinite classes of asymptotically good quasi-minimal codes by concatenation.

Theorem 3. *Let C be a linear $[n, k, d, d_{max}]_q$ code; if $d/d_{max} \geq (q-2)/(q-1)$, then C is quasi-minimal.*

Proof. Let C be a linear $[n, k, d]_q$ code and let c, c' be two linearly independent codewords of C such that $supp(c) = supp(c')$. Let α be a primitive element of $\mathbb{F}_q$. Then, w.l.o.g., one can write c and c' by blocks, in the following way: $c = \beta_0 || \ldots || \beta_{q-2} || 0$ and $c' = \alpha^0 \beta_0 || \ldots || \alpha^{q-2} \beta_{q-2} || 0$. Let

A_i be the size of the (possibly empty) block β_i. Then $wt(c) = wt(c') = \sum_{i=0}^{q-2} A_i \geq d$. We also have, for $j = 0, \ldots, q-2$, $d(\alpha^j c, c') = \sum_{i \neq j} A_i \geq d$. If we sum all these inequalities, we get $(q-2)\sum_{i=0}^{q-2} A_i \geq (q-1)d$, hence $wt(c) \geq \frac{q-1}{q-2}d > d_{max}$, a contradiction. Thus, c and c' cannot exist and C is quasi-minimal. □

Example 1. For $q = 3$, consider the code $G[11, 5, 6, 9]_3$ obtained by shortening the extended ternary Golay code([MS77]). It is quasi-minimal by the previous theorem. Its (Kronecker) square is G^2, a $[121, 25, 36, \geq 81]_3$ quasi-minimal code by the previous proposition, although is does not satisfy the sufficient condition of Theorem 3.

Now, the celebrated non-constructive Varshamov-Gilbert bound implies the existence of infinite families of semi-constructive quasi-minimal codes with rate $R = 1 - h_q(\frac{q-2}{q-1}) > 0$. This is still far from the upper bound, derived analogously to the minimal case:

Theorem 4 (Maximal Bound). *Let $\mathcal{C}$ be a quasi-minimal linear $[n, k, d]_q$ code, then $R \leq \log_q(2)$.*

3.4 Infinite constructions of quasi-minimal codes

Again, we concatenate a q-ary inner code (e.g. a simplex) with an infinite family of algebraic-geometric (AG) codes to get a high enough minimum distance and conclude by Theorem 3.

Continue taking for seed $\mathcal{S}_{q,r}[n = (q^r - 1)/(q-1), k = r, d = d_{max} = q^{r-1}]_q$, set $r = 2m$ and concatenate with $AG[N, K = NR, D = N\Delta]_{q^{2m}}$, obtaining the family $C[nN, kK, dD]_q$. Analogously to the minimal case, If $dD/d_{max}N = \Delta > (q-2)/(q-1)$, this family is quasi-minimal by Theorem 3.

Example 2.
- Take $q = 4, \mathcal{S}_{4,4}[85, 4, 64]_4, \Delta = 2/3 + \alpha, R = 4/15$, resulting in an infinite construction of $[n, 16n/1275]$ quaternary codes.
- For $q = 3$, we can improve on the simplex code seed: indeed, take the already considered $C[11, 5, 6, 9]_3$ as inner code and $AG[N, NR, N\Delta]_{3^5}$ with $R + \Delta = 191/208$. Choose $\Delta = 3/4, R = 35/208$; then concatenation results in an infinite construction of quasi-minimal $[n, \approx 0.076n]$ ternary codes.

4 Almost-minimal codes

Definition 5 (Almost-minimal linear code). *A linear code $\mathcal{C}$ is said (ϵ)almost-minimal if at most $q^{2\epsilon k}$ pairs of codewords are bad, for some fixed ϵ with $0 \leq \epsilon < 1/2$.*

We now extend some results of [CMP13] to almost-minimal codes.

Theorem 5 (Maximal Bound). *Let $\mathcal{C}$ an almost- minimal linear $[n, k, d]$ q-ary code, then $R \leq \log_q(2)/(1-\epsilon) + o(1)$.*

Proof. By definition, at most $q^{\epsilon k+1}$ codewords can share the same support. Thus, $|\mathcal{C}| = q^k \leq q^{\epsilon k+1} 2^n$ and $R = k/n \leq \log_q(2)/(1-\epsilon) + o(1)$.

Theorem 6 (Minimal Bound). *For any positive $R = k/n$ such that $R \leq \frac{1}{2-2\epsilon} \log_q(\frac{q^2}{q^2-q+1}) + o(1)$, there exists an infinite sequence of $[n, k]$ almost-minimal linear codes.*

Proof. Let us fix n and k. For $a \in \mathbb{F}_q^n$, such that $|supp(a)| = i$, there are $q^i - q$ linearly independent vectors b such that $supp(b) \subset supp(a)$. The pair (a, b) belongs to $\begin{bmatrix} n-2 \\ k-2 \end{bmatrix}$ linear $[n, k]$ codes, where $\begin{bmatrix} x \\ k \end{bmatrix}$ denotes the q-ary Gaussian binomial coefficient. There are less than $\sum_{i=0}^{n} \binom{n}{i}(q-1)^i(q^i - q) = (1 + (q-1)q)^n - q^{n+1} \leq (q^2 - q + 1)^n$ such ordered bad (a, b) pairs. As long as $q^{2\epsilon k} \begin{bmatrix} n \\ k \end{bmatrix} \geq \begin{bmatrix} n-2 \\ k-2 \end{bmatrix} (q^2 - q + 1)^n$, there are linear $[n, k]$ codes containing no more than $q^{2\epsilon k}$ bad pairs, *i. e.* almost-minimal codes. For $k/n \leq \frac{1}{2-2\epsilon} \log_q(\frac{q^2}{q^2-q+1}) + o(1)$, this quantity is positive.

Open problem

Is it true that the best achievable rate of (quasi, almost) minimal codes is a decreasing function of q? A weaker statement holds: if q divides q', then a q'- (quasi, almost) minimal code yields a q-ary (quasi, almost) minimal code with the same rate.

Acknowledgements

We thank Sasha Barg, Alain Patey and Zachi Tamo for helpful discussions.

References

[AB98] Alexei E. Ashikhmin and Alexander Barg. Minimal vectors in linear codes. *IEEE Transactions on Information Theory*, 44(5):2010–2017, 1998.

[BCS96] Gilles Brassard, Claude Crépeau, and Miklos Santha. Oblivious transfers and intersecting codes. *IEEE Transactions on Information Theory*, 42(6):1769–1780, 1996.

[CCP13] H. Chabanne, G. Cohen, and A. Patey. Towards Secure Two-Party Computation from the Wire-Tap Channel. *ArXiv e-prints*, June 2013.

[CELS03] Gérard D. Cohen, Sylvia B. Encheva, Simon Litsyn, and Hans Georg Schaathun. Intersecting codes and separating codes. *Discrete Applied Mathematics*, 128(1):75–83, 2003.

[CL85] Gérard D. Cohen and Abraham Lempel. Linear intersecting codes. *Discrete Mathematics*, 56(1):35–43, 1985.

[CMP13] G. Cohen, S. Mesnager, and A. Patey. On minimal and quasi-minimal linear codes. *Proceedings of Fourteenth International Conference on Cryptography and Coding, Oxford, United Kingdom, IMACC 2013, LNCS 8308 Springer, Heidelberg*, pages 85–98, 2013.

[DY03] Cunsheng Ding and Jin Yuan. Covering and secret sharing with linear codes. In Cristian Calude, Michael J. Dinneen, and Vincent Vajnovszki, editors, *DMTCS*, volume 2731 of *Lecture Notes in Computer Science*, pages 11–25. Springer DMTCS, 2003.

[Gil52] Edgar N. Gilbert. A comparison of signalling alphabets. *Bell System Technical Journal*, 31(3):504–522, 1952.

[Mas93] James L. Massey. Minimal codewords and secret sharing. In *Proc. 6th Joint Swedish-Russian Int. Workshop on Info. Theory*, pages 276–279, 1993.

[Mas95] James L. Massey. Some applications of coding theory in cryptography. In P. G. Farrell, editor, *Codes and Cyphers: Cryptography and Coding IV*, pages 33–47. Formara Ltd, 1995.

[MS77] F. J. MacWilliams and N. J. Sloane. *The theory of error-correcting codes*. Amsterdam, North Holland, 1977.

[Sch06] Hans-Georg Schaathun. The Boneh-Shaw fingerprinting scheme is better than we thought. *IEEE Transactions on Information Forensics and Security*, 1(2):248–255, 2006.

[SL12] Yun Song and Zhihui Li. Secret sharing with a class of minimal linear codes. *CoRR*, abs/1202.4058, 2012.

[TV91] Michael A. Tsfasman and Serge G. Vladut. *Algebraic Geometric Codes*. Kluwer, 1991.